LISTING OF CLAIMS

The following is a copy of Applicant's claims that identifies language being added with underlining ("___") and language being deleted with strikethrough ("~~___~~"), as is applicable:

1. (Currently Amended) A method of passing data securely from an originator to a recipient comprising the steps of:

the originator selecting a condition that the recipient must meet for receipt of the data;

the originator selecting a trusted party;

the originator selecting a first key without reference to the condition;

the originator encrypting the data using the first key;

the originator making the condition, and the encrypted data available to the recipient;

the recipient providing the trusted party with evidence that it meets the condition;

the trusted party satisfying itself that the recipient does meet the condition and providing the first key to the recipient, and

the recipient decrypting the data using the first key.

2. (Original) A method according to claim 1 wherein the trusted party has an asymmetric key pair comprising a public key and a private key, of which the public key is known, and the method includes the additional steps of:

the originator encrypting the condition and the first key using the public key of the trusted party;

the originator making the encrypted condition and first key available to the recipient;

the recipient forwarding the encrypted condition and first key to the trusted party, with the proof that it meets the condition, and

the trusted party decrypting the condition and first key using its private key and satisfying itself that the recipient meets the condition.

3. (Original) A method according to claim 2 wherein the recipient has an asymmetric key pair comprising a private key and a public key and the method includes the additional steps of:

the recipient providing its public key to the trusted party;

the trusted party encrypting the first key with the recipient's public key and then transmitting it to the recipient, and

the recipient decrypting the first key using it's private key before using it to decrypt the data.

4. (Original) A method according to claim 2 wherein the first key is an asymmetric key pair, of which the encrypting first key is used to encrypt the data and the decrypting first key is encrypted with the condition using the public key of the trusted party.

5. (Original) A method according to claim 1 wherein the selection of the first key comprises the originator requesting it from the trusted party which generates an asymmetric key pair and provides the encrypting key of the asymmetric key pair to the originator to act as an encrypting first key; and

the method includes the additional steps of:

the originator providing the condition to the trusted party;

the trusted party storing the condition and the asymmetric key pair;

the recipient providing the trusted party with evidence that it meets the condition;

the trusted party retrieving the condition and asymmetric key pair from store, and satisfying itself that the recipient meets the condition, and

the trusted party providing the decrypting key of the asymmetric key pair to the recipient to act as a decrypting first key.

6. (Original) A method according to claim 5 wherein it includes the additional steps of:

the trusted party encrypting the decrypting first key with the recipient's public key before transmitting it to the recipient, and

the recipient decrypting the decrypting first key before using it to decrypt the data.

7. (Original) A method according to claim 1 wherein at the time the originator encrypts the data the recipient is unknown to them.

8. (Original) A method according to claim 1 wherein the step of the originator making available the condition and the encrypted data involves publishing or storing it for later collection by the recipient.

9. (Original) A method according to claim 8 wherein the step of the originator making available the condition and the encrypted data involves saving it onto a physical storage medium for later collection by the recipient.

10. (Original) A method for an originator to make data available securely to a recipient comprising the steps of:

the originator selecting a condition that the recipient must meet for receipt of the data;

the originator selecting a trusted party;

the originator selecting a first key without reference to the condition;

the originator encrypting the data using the first key, and

the originator making the condition, and the encrypted data available to the recipient.

11. (Original) A method according to claim 10 wherein the trusted party has an asymmetric key pair comprising a public key and a private key, of which the public key is known, and the method includes the additional steps of:

the originator encrypting the condition and the first key using the public key of the trusted party, and

the originator making the encrypted condition and first key available to the recipient.

12. (Original) A method according to claim 11 wherein the first key is an asymmetric key pair, of which the encrypting first key is used to encrypt the data and the decrypting first key is encrypted with the condition using the public key of the trusted party.

13. (Original) A method according to claim 10 wherein the selection of the first key comprises the originator requesting that the trusted party generates an asymmetric key pair and provides the encrypting key of the asymmetric key pair to the originator to act as an encrypting first key; and

the method includes the additional step of the originator providing the condition to the trusted party.

14. (Original) A method for a recipient to receive data made available securely by an originator, who has selected a trusted party to be involved, comprising the steps of:

obtaining a condition for decryption of the data set by the originator and the data encrypted using a first key generated without reference to the condition and;

providing the trusted party with evidence that it meets the condition;

receiving the first key for decryption of the data from the trusted party, and

decrypting the data.

15. (Original) A method according to claim 14 wherein the trusted party has an asymmetric key pair comprising a public key and a private key, of which the public key is known and was used by the originator to encrypt the condition and first key, and the method includes the additional steps of:

obtaining in encrypted form the condition and first key made available by the originator, and

forwarding the encrypted condition and first key to the trusted party, with the evidence that it meets the condition.

16. (Currently Amended) A method according to claim 15 wherein the recipient has an asymmetric key pair comprising a public key and a private key, and the method includes the additional steps of:

providing the trusted party with ~~the~~ its public key;

receiving from the trusted party the first key encrypted with the ~~recipients~~ recipient's public key, and

decrypting the first key using its private key prior to using the first key to decrypt the data.

17. (Currently Amended) A method for a trusted party to facilitate the passing of data securely from an originator to a recipient, where the originator has selected a condition which the recipient must meet for receipt of the data, and has encrypted the data with a first key generated without reference to the condition, comprising the steps of:

receiving from the recipient evidence that they meet the condition;

comparing the evidence against the condition to confirm that the recipient does meet the condition, and

if the recipient meets the condition, providing the first key to the recipient that is capable of decrypting the data.

18. (Original) A method according to claim 17 wherein the trusted party has an asymmetric key pair comprising a public key and a private key, of which the public key is known, and the method includes the additional steps of:

receiving from the recipient the condition and first key encrypted using the public key of the trusted party;

decrypting the condition and first key using the private key of the trusted party prior to comparing the evidence against the condition to confirm that the recipient does meet the condition.

19. (Original) A method according to claim 18 wherein it includes the additional steps of:

receiving from the recipient its public key;

encrypting the first key with the recipient's public key, and

transmitting the encrypted first key to the recipient.

20. (Original) A method according to claim 18 wherein the first key is an asymmetric key pair.

21. (Original) A method according to claim 17 wherein the trusted party is requested by the originator to generate an asymmetric key pair to act as the first key and once the asymmetric key pair has been generated the encrypting first key is provided to the originator, and the method includes the additional steps of:

receiving the condition from the originator;

storing the condition and the asymmetric first key pair;

upon receipt of the evidence from the recipient that they meet the condition, retrieving the condition and asymmetric first key pair from store before comparing the evidence against the condition to confirm that the recipient does meet the condition, and

providing to the recipient the decrypting key of the asymmetric first key pair to act as a decrypting first key.

22. (Original) A method according to claim 21 wherein it includes the additional step of encrypting the decrypting first key with the recipient's public key before transmitting it to the recipient.

23. (Original) A computer system for implementation of the method of claim 1.

24. (Original) A computer system for implementation of the method of claim 10.

25. (Original) A computer system for implementation of the method of claim 14.

26. (Original) A computer system for implementation of the method of claim 17.

27. (Original) A computer system for passing data securely from an originator to a recipient comprising a first computer entity associated with the originator, a second computer entity associated with the recipient and a third computer entity associated with a trusted party, there being communication means between the first computer entity and the second computer entity and between the second computer entity and the third computer entity,

the first computer entity selecting a condition to be met by the recipient before receipt of the data and a first key generated without reference to the condition, and encrypting the data with that first key, and encrypting the condition and the first key using a public key of the trusted party, and making both available to the second computer entity;

the second computer entity being arranged to forward evidence that the recipient meets the condition to the third computer entity, and

the third computer entity being arranged to compare the evidence with the condition and if satisfied that the recipient meets the condition to provide the first key to the second computer entity for decryption of the data.

28. (Original) A computer system according to claim 27 wherein the trusted party has a public key and:

the first computer entity is arranged to encrypt the condition and the first key using the trusted party's public key and make that available to the second computer entity,

the second computer entity is arranged to forward the encrypted condition and first key to the third computer entity, and

the third computer entity is arranged to decrypt the condition and first key before comparing the evidence with the condition.

29. (Currently Amended) A computer system according to claim 28 wherein:

the second computer entity is arranged to provide a public key of the recipient to the third computer entity, and

the third computer entity is arranged to encrypt the first key with the ~~recipients~~ recipient's public key before transmitting it to the recipient.

30. (Original) A computer system according to claim 27 wherein:

the first computer entity is arranged to provide the condition to the third computer entity,

the third computer entity is arranged to generate an asymmetric first key pair and to provide the encrypting first key to the first computer entity, and

the second computer entity is arranged to provide the third computer entity with the condition and the evidence.

31. (Original) A method of passing data securely from an originator to a recipient comprising the steps of:

the originator selecting a condition that the recipient must meet for decryption of the data; the originator selecting a trusted party having a public key;

the originator selecting a first key without reference to the condition;

the originator encrypting the data using the first key;

the originator encrypting the condition and the first key using the public key of the trusted party;

the originator making the condition, and the encrypted data and the encrypted condition and first key, available to the recipient;

upon receipt by the trusted party of the recipient's public key, the encrypted condition and first key, and evidence that the recipient meets the condition, the trusted party decrypts the condition and first key, satisfies itself that the recipient meets the condition, provides the first key to the recipient, and

the recipient decrypts the data using the first key.

32. (Original) A method of passing data securely from an originator to a recipient comprising the steps of:

the originator selecting a condition that the recipient must meet for decryption of the data;

the originator selecting a trusted party;

the trusted party generating an asymmetric key pair without reference to the condition and providing the encrypting key of the asymmetric key pair to the originator to act as a first encrypting key;

the originator providing the condition to the trusted party;

the trusted party storing the condition and the asymmetric key pair;

the originator encrypting the data using the first encrypting key;

the originator making the condition, and the encrypted data available to the recipient;

upon receipt by the trusted party from the recipient of the evidence that the recipient meets the condition the trusted party retrieves the condition and asymmetric key pair from store, satisfies itself that the recipient meets the condition, and provides the decrypting key of the asymmetric key pair to the recipient to act as a first decrypting key, and

the recipient decrypting the data using the first decrypting key.